Computer User Security Training

Army Logistics Management College

Agenda

1. Objectives
2. Introduction
3. Lesson 1 - 8
4. Summary
5. Signing the AUP

Objectives

- Effective physical security of computer hardware and software.
- Limit access to computer equipment to authorized users only.
- Prevent computer fraud, waste and abuse.
- Implement effective contingency planning.
- Report security problems to the chain of command.
- Protect computer files from infection by malicious logic.

Introduction

- Information Technology (IT) has enabled the Department of Defense (DoD) to transmit, communicate, collect, process, and store unprecedented amounts of information. Increasing dependence on Information Systems (IS) has focused attention on the need to ensure that these assets, and the information they process, are protected from actions that would jeopardize the Department of Defense's ability to effectively function. Responsibility for securing this information and its systems lies with the components.

Lesson 1

- The trained and aware individual employee is the first and most vital line of defense in protecting DoD information and IS.
- DoD IT users shall maintain a degree of understanding about Information Assurance (IA) policies and doctrine commensurate with their responsibilities.
- DoD employees with access to IT are required to receive both initial and annual refresher IA awareness training.
- As a user of a Government Computer (GC), your actions can greatly affect the security of our networks.
- Awareness training shall be current.
- Before you can be issued a permanent username and password, you must sign the Acceptable Use Policy (AUP).

Lesson 2

- Most GCs are networked, your GC can reach or be reached by almost every unclassified GC in DoD.
- Almost all GCs on the Non-secure Internet Protocol Router Network (NIPRNET) are linked to the commercial Internet.
- The Secret Internet Protocol Router Network (SIPRNET) is used to link DoD GCs together to share classified information up to secret. It is not however; connected to the commercial Internet.
- DoD GC have access to vast amounts of information exposing DoD's GCs to risks from all computers to which it can be linked.
- As a user of a GC, you play a key role in protecting our data.

Lesson 3

- Threats to your GC come from a virus, hacker, or even from a soldier or DoD civilian in the military or U.S. Government or contractors.
- Viruses and worms are programs that corrupt and damage programs, data, or both. The program does not have to perform malicious actions to be a virus or a worm; it only needs to infect or alter other programs.
- Opening an infected e-mail message or attachment from a known or an unknown source is the most common method viruses are spread today.
- You should never configure your computer to automatically preview e-mail messages.
- Deliberately introducing “malicious logic” (the technical term for viruses and other malicious programs) into any Government information system is a Federal crime.

Examples of Internal Threats

- Malicious/incompetent insiders
- Viruses (Trojan Horse, Bomb, Worms)
- Insiders in the employ of terrorist groups or foreign countries
- Disgruntled employee/service members
- Hackers
- Crackers
- Self-inflicted intentional or unintentional damage

Examples of External Threats

- Script kiddies
- Crackers
- Hackers
- Protesters
- Agents in the employ of terrorist groups or foreign countries
- Viruses (Trojan Horse, Bombs, Worms)
- Acts of nature

Prevention

- Ensure anti-virus software on your GC is current.
- Be aware and report unusual computer activity.
- Log off your computer at the end of the day if the computer is remaining in the building overnight. DO NOT POWER IT OFF (notebook lids should remain open).
- Scan government issued thumb drives for viruses each morning when you return to class **(Double click on MY COMPUTER, find the drive designated for the thumb drive, right click on it and click on "Scan for Viruses…")**

Things to look for

- Abnormal displays or banners appear on the computer screen.
- The computer’s performance slows down.
- The computer shows unusual activity or displays error messages, file sizes change, or data or programs are lost.

Lesson 4

- GC are to be used by Government employees for official business, authorized personal use, and limited morale and welfare communications between deployed soldiers and their family members.

Lesson 4

- Safeguard each information system and its information against sabotage, tampering, denial-of-service, espionage, and release of unauthorized persons.
- Protect hardware, software, and documentation at the highest classification of the information residing on the information system.
- Report information systems security incidents, vulnerabilities, and virus attacks.
- Check all government issued magnetic media (disks, CDs, tapes) for malicious software (viruses, worms) before using it on a GC, IT system or network.

Lesson 4

- Personal use of a GC is authorized when it-
  - Conforms to DoD policy.
  - Is of reasonable duration and frequency and, when possible, is done before or after normal duty hours.
  - Does not create significant additional costs to DoD, and does not reflect adversely on DoD.
  - Serves a legitimate public interest, such as furthering the education and self-improvement of employees or improving employee morale and welfare.
  - Does not overburden the military communication system. Remember, the military communication system is designed to support the mission requirements of the war-fighter.

Lesson 4

- Although the Common Access Card (CAC) with your Personal Identification Number (PIN) is the principle authenticator for the government network, passwords are still required for access to many sites, such as ALMC, or certain applications.
- Maintaining the security of your password is therefore one of the most important security precautions you must take as a user.
- You are responsible for any activity that takes place on a GC under your logon name and password.

Lesson 4

- The guidelines below will help you protect your password.
  - Do not write down or post your password in your classroom or work area.
  - Do not store your password on-line or in a PDA or PED, and do not include it in e-mail messages.
  - Make sure your password is not exposed on the screen when you log in.
  - If you know your password is compromised, contact the ALMC ITO Help Desk in room B-118.

Lesson 4

- Authorized Software and Hardware
  - Software and Hardware used on GC must be licensed, accredited, and approved by your commander, IASO, and IMO.
  - You may not load any software on your GC or install or connect any hardware (including PDAs, USBs, and PEDs) on a network without first obtaining written approval from ALMC's IASO, SA, or IMO.
  - All PDAs and PEDs (personal or Government-owned) must be loaded with DoD-approved, anti-virus software.

Lesson 4

- Soldiers, civilians, and contractors who are authorized e-mail accounts are required to have an AKO web-mail account. All other web-mail services are prohibited for business communications. AKO also provides the only authorized Internet chat service allowed on the NIPRNET; all other chat services are prohibited.

Prohibited Activity

- Having or Loading Prohibited Software:
  - Peer-to-peer file-sharing software, commonly used to share copyrighted materials such as MP3 music and video files
  - Hacker tools and development software
  - Malicious logic and virus-development software
  - Network line-monitoring and keystroke-monitoring tools
  - Unlicensed (pirated) software
  - Webpage-altering software
  - Games
  - Personal firewalls (including DoD licensed and Windows XP Internet connection firewall)

Prohibited Activity Continued

- Using commercial Internet chat service such as AOL, Instant Messenger, Yahoo chat, and websites that promote chat services.
- Using networked IT or GCs for personal gain or illegal activities.
- Attempting to strain, test, circumvent, or bypass computer-network or security controls.
- Attempting to access data or use operating systems or programs, except as specifically authorized.
- Performing network line-monitoring or keystroke-monitoring without proper authorization.
- Modifying or tampering with the software or hardware on your GC without proper authorization.
- Moving your GC without your SA, IASO, or IMO's approval. Most damage to computers occurs when moving them.

Prohibited Activity Continued

- Introducing viruses, worms, or malicious codes into any IT or network.
- Sharing user-identification or passwords.
- Storing, processing, displaying, sending, or otherwise transmitting offensive or obscene material, such as racist, sexually explicit, harassing, or hate literature.
- Storing or processing classified information on a system (including PEDs and PDAs) not approved for classified processing.
- Storing or processing copyrighted material (including cartoons) unless approval is obtained from the author or publisher.
- Viewing, changing, damaging, deleting, or blocking access to another user's files or communications.
- Obtaining, installing, copying, storing, or using software in violation of the appropriate vendor's license agreement.

Prohibited Activity Continued

- Giving an unauthorized individual access to a Government-owned or Government-operated system.
- Hacking into or from the DoD network.
- The use of commercial ISP (for example: CompuServe, AOL, Prodigy) or email accounts for official purposes.
- Auto-forwarding of official mail to non-official accounts or devices.
- Using someone else's user identification and password or masking your identity.
- Installing and using a modem without approval from your DAA.
- Writing or forwarding chain or hoax e-mail messages.
- Posting personal homepages.
- Using a GC for personal profit.
- Downloading or loading freeware or shareware software.
- Simultaneously connecting to a Government network and a commercial ISP.
- Simultaneously connecting to the NIPRNET and a commercial ISP with a PED or PDA modem.

Consent to Auditing and Monitoring

- All transactions by users accessing the NIPRNET or SIPRNET are subject to audit.
  - Auditing is defined as the independent review and examination of records and activities to assess the adequacy of system performance and controls, to ensure compliance with established policy and operational procedures, and to recommend necessary changes in controls, policy, or procedures.

Consent to Auditing and Monitoring

- When you click OK on the warning banner that appears when you start your GC, you are agreeing to have your GC monitored.
  - Monitoring is used for surveillance, to reconstruct account activity, and to record attempts to bypass security mechanisms.

Minimize Policy

- During periods of heightened network activity, your installation may be forced to minimize non-mission-essential activity on our networks. When MINIMIZE order is issued to all users of computer networks in the Army, all personal use of GCs is prohibited for the duration of the order, except for the following:
  - E-mail messages between deployed soldiers and their families.
  - GC use required for DoD or other authorized education-center training or programs leading to college degrees.
  - Morale, welfare, and recreation activities.
  - Department of Defense Dependent Schools (DODDS) activities, provided student activity is monitored by adult supervisors.

Lesson 5

- If you think you have observed a computer security incident, you must report it to your SA or IASO immediately. A few examples of computer security incidents are as follows:
  - Attempts (either failed or successful) to gain unauthorized access to a system or its data (for example hacking).
  - Attempts (either failed or successful) to defeat or circumvent computer-network or security controls (for example WebSense, Passwords).
  - Downloading MP3 files or other unauthorized software.
  - Writing or knowingly transmitting a virus, worm, or other forms of malicious logic.
  - Forwarding chain e-mail messages.

Lesson 5

- Immediately inform your SA or IASO if you think –
  - Your GC has a virus.
  - Your government issued thumb drive has a virus or any unknown files present.
  - Your GC has been hacked or is being hacked.
  - An unauthorized or required activity on the network is not functioning correctly.
  - Do not turn off your GC.
  - Disconnect the network cable from the GC.
  - Call your SA or IASO.

Lesson 6

- You must treat your GC with care for it to function properly.
  - Do not eat or drink near your GC.
  - Keep your system clean and free of dust.
  - Never disconnect your GC from its network-connection box (unless you think it is infected).
  - Do not move your GC unless directed by your Course Director, SA, or IASO.
  - Log off your computer at the end of the day.
  - Log off any publicly available computer (such as the Information Center in the C-Wing or the Simulation Rooms in the A-Wing) when you finish; never lock the computer.

Lesson 7

- The Computer Fraud and Abuse Act (18 U.S. Code 1030, Public Law 99-474) was passed in 1986 to combat what is now commonly known as “hacking”. Any federal agency and/or the Secret Service is authorized to investigate any offensive under this act. The list below is what is considered illegal under this act.
  - Knowingly access without authorization any computer system and in doing so obtain restricted or classified government information.
  - Knowingly access without authorization any computer system, and in doing so obtain financial information held by a financial institution, credit information held by a consumer reporting agency, or credit card information held by the issuer of credit cards.

Lesson 7 Continued

- Intentionally and without authorization access any computer of a department or agency of the United States if the computer is exclusively for use, or if not exclusively for use, in a way that affects the government's use of the computer.

- Knowingly, and with intent to defraud, traffic in any password or similar information through which a computer can be accessed without authorization if such trafficking affects interstate or foreign commerce or such computer is used by the government of the United States.

Lesson 7 Continued

- Electronic Communications Privacy Act of 1986 (ECPA) Public Law 99-508 begun as an “anti-wiretapping” act, the ECPA was meant to combat the eavesdropping problems presented by such events as the Watergate scandal in the early 1970’s. The law was modified to deal with all forms of digital communications, including transmission of text and digitized images, as well as telephone communications.
  - Applicability
    - The CPA prohibits unauthorized eavesdropping by all persons, businesses, and the government.

Lesson 7 Continued

- Warning for Administrators
  - The ECPA prohibits unauthorized access to messages in storage on computer systems and the unauthorized interception of messages in transmission.

- Prohibitions on wire, oral, and electronic communications.
  - Prohibits interception and disclosure
  - Prohibits interception devices
  - Prohibits the use as evidence of communications

Lesson 7 Continued

- Interception requires authorization by federal judge.

- Lawful monitoring.
  - A provider of wire or electronic communication service can intercept, disclose, or use that communication if
    - It is necessary to rendering the service.
    - It is necessary for the protection of the service provider’s property or rights.
    - This is meant to protect the provider and the user of that service.

Lesson 7 Continued

- Unlawful monitoring
  - A provider of wire communication service cannot utilize service observing or random monitoring except for mechanical or service quality control checks.

- Additional reading:
  - You are invited to read the article, Legal Issues, A Site Manager's Nightmare, by Stephen E. Hansen, Stanford University, at the JANET-CERT web site of the UK Academic Research Center.

Lesson 7 Continued

- Computer Security Act of 1987, Public Law 100-235
  - Most states provide for criminal prosecution in cases of:
    - Unauthorized use of or access to a computer.
    - Destruction, modification, or alteration of data or computer programs.
  - Additional (not required reading).
    - Georgia Computer Systems Protection Act.

Lesson 8

- Wireless Security Risks
  - A wireless LAN can be thought of as two or more unwired computers using the airwaves with the help of an access point.
  - The improper use of wireless networks within the Army can needlessly expose the network to additional vulnerabilities that are not present in the wired LAN.

Lesson 8 Continued

- Known vulnerabilities of a wireless network:
  - Default configuration settings are known to hacker community.
  - User authentication not required for access.
  - Wireless networks have no set physical boundaries.
  - Access points are often located in exposed locations.
  - Untrained users setting up unauthorized workstations and networks.
  - Unauthorized access points.
  - Lack of network monitoring.
  - Poor network performance.
  - Inadequate or no encryption.
  - Supports eavesdropping.
  - Unsecured holes in the network.
  - Denial of Service attacks.

Lesson 8 Continued

- Wireless vulnerabilities prevention:
  - All changes to the network must be authorized and accredited.
  - All modifications to the network should be done by trained network personnel.
  - Adding personal or non-ALMC issued wireless devices to the network is forbidden.
  - Do not take wireless devices into restricted security environments.
  - If you see an unsafe network condition, report it to your SA or IASO.

Summary

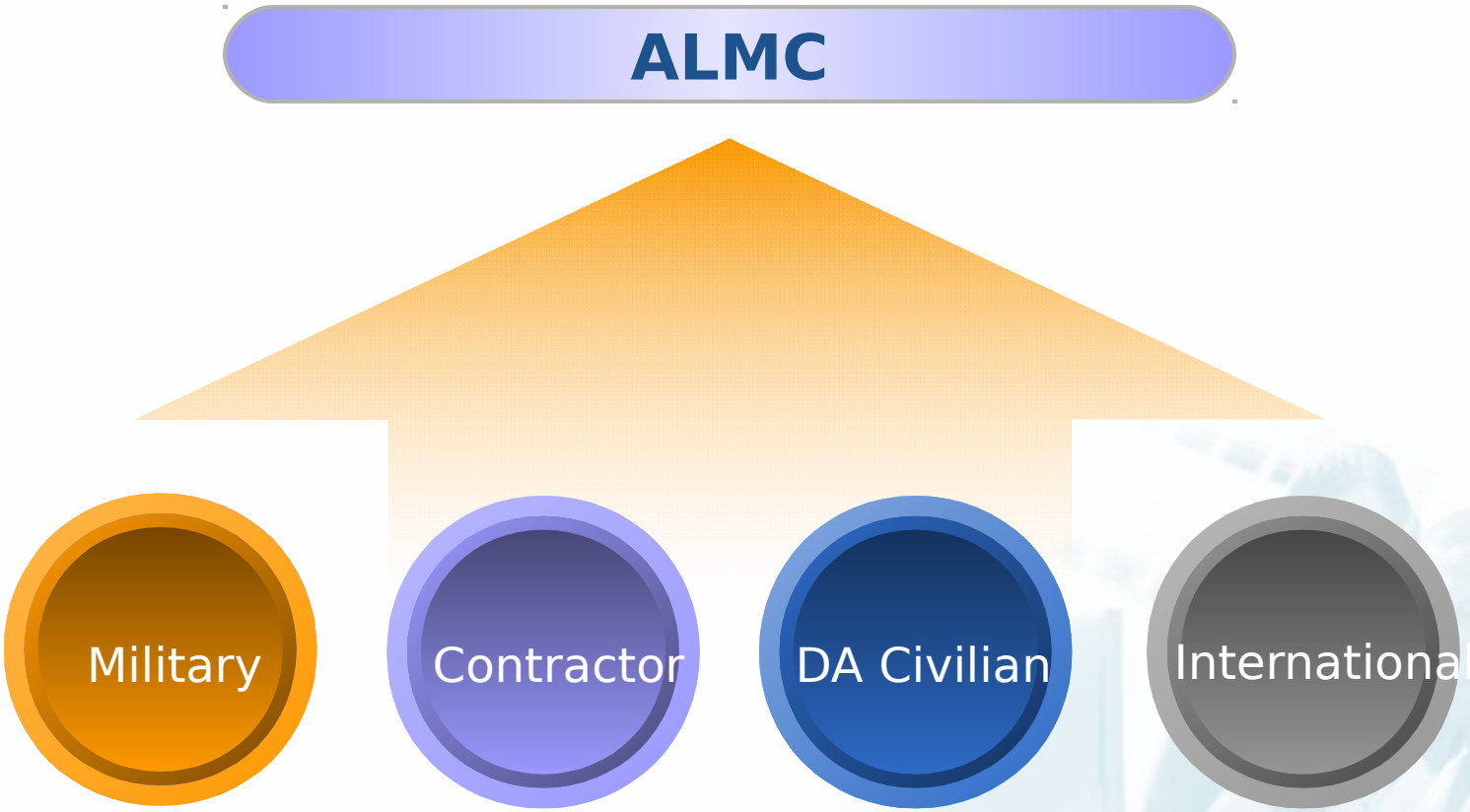
- As a GC user, you play a key role in protecting the integrity, availability, and confidentiality of data.
  - Guard your password
  - Ensure your anti-virus software is up-to-date
  - Follow the rules on personal use of the computer
  - Report viruses and all other network-security incidents to your SA or IASO

Sign the AUP

- Before you receive a log-on name and password for your GC, your IMO or IASO will require you to read and sign the Acceptable Use Policy (formerly Computer User Agreement).

- Your signature acknowledges your understanding of and agreement to support policy on the use of GCs. Your signature also makes you accountable for every transaction that occurs on your GC account.

Working together



UNCLASSIFIED